Journal of Computer and System Sciences 78 (2012) 1703–1715

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Improvement of assurance including security for wireless sensor networks using dispersed data transmission

Eitaro Kohno [a,*], Tomoya Okazaki [a], Mario Takeuchi [a], Tomoyuki Ohta [a], Yoshiaki Kakuda [a], Masaki Aida [b]

[a] *Graduate School of Information Sciences, Hiroshima City University, 3-4-1, Ozuka-Higashi, Asaminami-Ku, Hiroshima 731-3194, Japan*
[b] *Graduate School of System Design, Tokyo Metropolitan University, 6-6, Asahigaoka, Hino-shi, Tokyo, 191-0065, Japan*

ARTICLE INFO

Article history:
Received 31 January 2011
Received in revised form 16 May 2011
Accepted 28 October 2011
Available online 3 December 2011

Keywords:
Wireless sensor networks
Node capture attacks
Multipath routing
Assurance

ABSTRACT

Assurance networks are one of the essential technologies of New-generation Networks. Assurance is defined as the capability of guaranteeing functional and non-functional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing requirements. Assurance is essential for sustainable networks and this research focused specifically on providing assurance for WSNs. Node capture attacks are one prospective kind of attack on WSNs. To reduce negative effect of node capture attacks, we have previously proposed secure decentralized data transfer. In this proposed method, it was assumed that multiple paths were in place. In this paper as well, we again propose using the multipath routing method. To make multiple paths fit our previously proposed method, we have modified ATR (Augmented Tree Based Routing). We have conducted simulation experiments using our proposed method in a network simulator. The results show that our previously proposed method is effective in both cases in which the network size is small or large. In addition, we conducted other simulation experiments to measure several aspects of the assurance of our method. We measured in terms of varying parameters such as node densities, distance between the source and the destination nodes, and so on. Additionally, our method is more assured than the single path-based method.

1. Introduction

Wireless sensor networks (WSNs) [1,2] are an important direction for future networks. Disaster response, weather observation, crime prevention, and healthcare systems are examples of applications where WSNs are utilized. The size of WSNs varies a great deal depending on the usage. WSNs consist of tiny nodes and sink nodes. Data on WSNs are transferred by wireless links. When a node (a source node) cannot communicate with the sink node (the destination node), intermediate nodes relay data from the source to the destination. This act of relaying data is referred to as multi-hop communication. Tiny nodes are deployed on the object or in the field to collect measurements. Because the nodes are small they have severely limited memory size and computational power. They are deployed in a possibly hostile environment in which several kinds of attacks may occur. Node capture attacks are one prospective kind of attack on WSNs [3]. To prevent such attacks, several existing methods have been proposed. TinySec [4] is a security architecture used to ensure confidentiality when transferring data. TinySec uses a symmetric key such as RC4. While TinySec can protect data using key based cryptography, it is weak against node capture attacks. When a node is captured, adversaries can get the key of the cryptosystem and all of the data of the node. Since TinySec uses one common key for the system, adversaries can get all of the data in the network using

[*] Corresponding author.
E-mail address: kouno@hiroshima-cu.ac.jp (E. Kohno).

0022-0000/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcss.2011.10.018

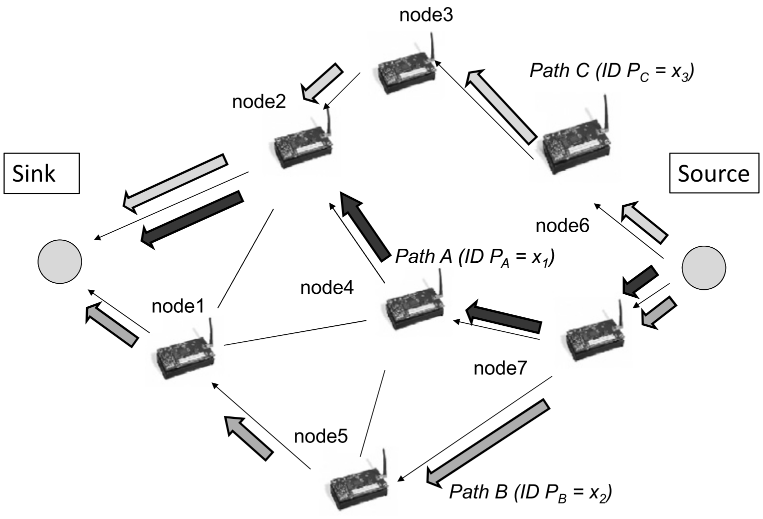

Fig. 1. Secure decentralized data transfer against node capture attacks.

the stolen key. To counter this, asymmetric key-based systems have been proposed. They are effective in limiting damage against attacks. When a secret key is captured in symmetric key-based and asymmetric key-based systems, those systems have to change the pair of keys. To do that, a random key pre-distribution scheme [5] and its successor [6,7] have been proposed. Those systems need to send control packets to create keys. These results in a large delay before data can be transmitted. That waiting time becomes long in large networks.

We have proposed a new method to protect data security against node capture attacks using distributed data transfer [8]. To use this method, we have to establish multiple paths. In the past we proposed a scalable method to create multiple paths for distributed data transfer with a small number of control packets [9]. In that same paper, we implemented the proposed method in the simulator by conducting simulation experiments on small and large networks and confirmed the effectiveness of the method on both. This proposed method was designed to hold up against changing environmental parameters such as the node density, the number of source nodes, and the hop length between sources and the destination. In real systems, the resiliency in light of those varying parameters will be important. *Assurance* or *assurance networks* express that resiliency. According to [10], assurance in distributed systems and networks is defined as the capability of guaranteeing functional and non-functional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing requirements. Networks which have the aforementioned assurance are defined as *assurance networks*. Assurance network technologies are important for *New-generation networks*, which Japan's National Institute of Information and Communication Technology plans to research. In the literature [11], Avižienis et al. proposed the concept of dependability. They claimed that simultaneous consideration of dependability and security provides a very convenient means of subsuming various concerns within a single conceptual framework. Assurance is one framework that looks into faults and security. In this paper, we propose a method to evaluate both the security aspect of assurance, by focusing on confidentiality, and the dependability aspect, by focusing on resiliency against node faults.

The rest of the paper consists of the following: In Section 2, we introduce the dispersed data transfer method, which has been proposed to hinder node capture attacks. In Section 3, we describe our new method. In Sections 4 and 5, we illustrate our experiments and discuss the results. We conclude the paper in Section 6.

2. Secure decentralized data transfer against node capture attacks

In wireless sensor networks (WSNs), tiny sensor nodes are deployed on the object or to the field to collect measurements. A tiny sensor node has limited resources such as the available CPU power and the memory size.

In addition, the field to be measured is a possibly hostile environment for WSNs in many cases. The tiny sensor nodes are deployed and work autonomously for a certain period of time. It is not feasible for each sensor node to have detecting capabilities to sense adversaries. To cope with security problems in WSNs, many countermeasures have been proposed. Although many of them are key-based systems, the protection of the secret key(s) is a serious concern. When secret keys are stolen by way of node capture attacks, encrypted data can be decrypted by adversaries. In the past, we have proposed a method to secure decentralized data transfer against node capture attacks [12,8] (hereafter referred to as the previously proposed method). Fig. 1 shows the data transfer of our previously proposed method. The previously proposed method can encrypt data being transferred using the secret-sharing-scheme-based data dispersion [13,14,12]. In the literature [12], we can confirm the effectiveness of our previously proposed method using small size networks consisting of about nine nodes.

Assurance in these distributed systems and networks is defined as the capability of guaranteeing functional and non-functional system properties such as dependability, security, timeliness and adaptability to heterogeneous and changing